911 Reliability and the Challenges of an Evolving Ecosystem

October 27, 2016

Federal Communications Commission

Making **Connections that Matter®**

COMTECH TELECOMMUNICATIONS CORP.

Agenda

- The Role of Hosted 911 Service Providers
- IP-based 911 and the Vulnerabilities of the Public Internet
- Distributed Denial of Service (DDoS) Attacks
  - Overall Status in North America
  - A 911 Case Study
  - Remediation Status

The Role of Hosted 911 Service Providers

- With legacy networks, the responsibility for routing 911 calls belongs to the incumbent telephony providers in a given market – typically the local exchange carriers

- Deregulation of telecom, first in the 1970's and then more fully in the mid-1990's, brought increased competition and the fracturing of the 911 ecosystem

- The result was an evolution to a more complex landscape for service providers - one that included new offerings, such as hosted or managed services

- Today Comtech provides 911 services to approximately **150 different customers**, serving over **300 million end user access points** across **thousands of geographic markets** (states, counties, PSAPs, etc.)

IP-based 911 and the Vulnerabilities of the Public Internet

- In the legacy 911 networks, little if any 911 traffic – voice traffic, location determination data, PSAP routing data – was transmitted over the Public Internet
- By 2003, emergency "i2" VoIP shifted the traditional wireline 9-1-1 paradigm towards NG9-1-1
- The increasing number of NG9-1-1 technologies – including IP-based ESInets and Next Generation Core Services – are the vanguard to the all IP-based 911 infrastructure of the future
- With progress being made towards far greater network capabilities and significantly increased value to consumers, so too comes greater risks and vulnerabilities
- The challenge for service providers and regulators is to moderate the risk while fostering innovation in Public Safety

IP-based 911 and the Vulnerabilities of the Public Internet

- Limited points of ingress into traditional 911 networks significantly limits potential attack vectors, with insider attacks representing the greatest threat.

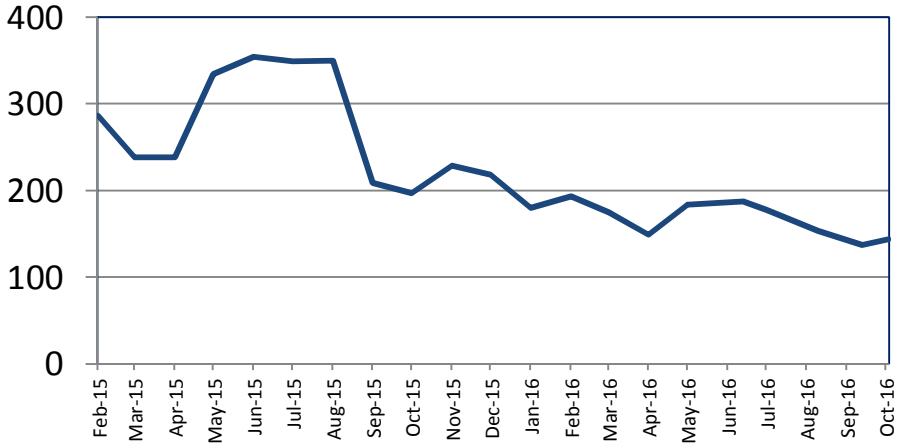
- However, an Internet-connected infrastructure exposes 911 services to a wide range of skilled and generally anonymous threat actors including criminals, hackers, activists, anarchists, rogue nation states and terrorists.

- Aggressive attack vectors can disrupt or disable 911 leading to:
  - **COMPROMISED CONFIDENTIALITY** – By exposing sensitive personal and logistical information.
  - **DIMINSHED INTEGRITY** – By undermining public trust in the national 911 system.
  - **LOSS OF LIFE** – By disrupting or eliminating emergency response.

IP-based 911 and the Vulnerabilities of the Public Internet:

Text-to-9-1-1 deployment data provides some insight regarding internet-related risks

Text-to-911 Deployments in Progress



Text-to-911 Deployments by Type

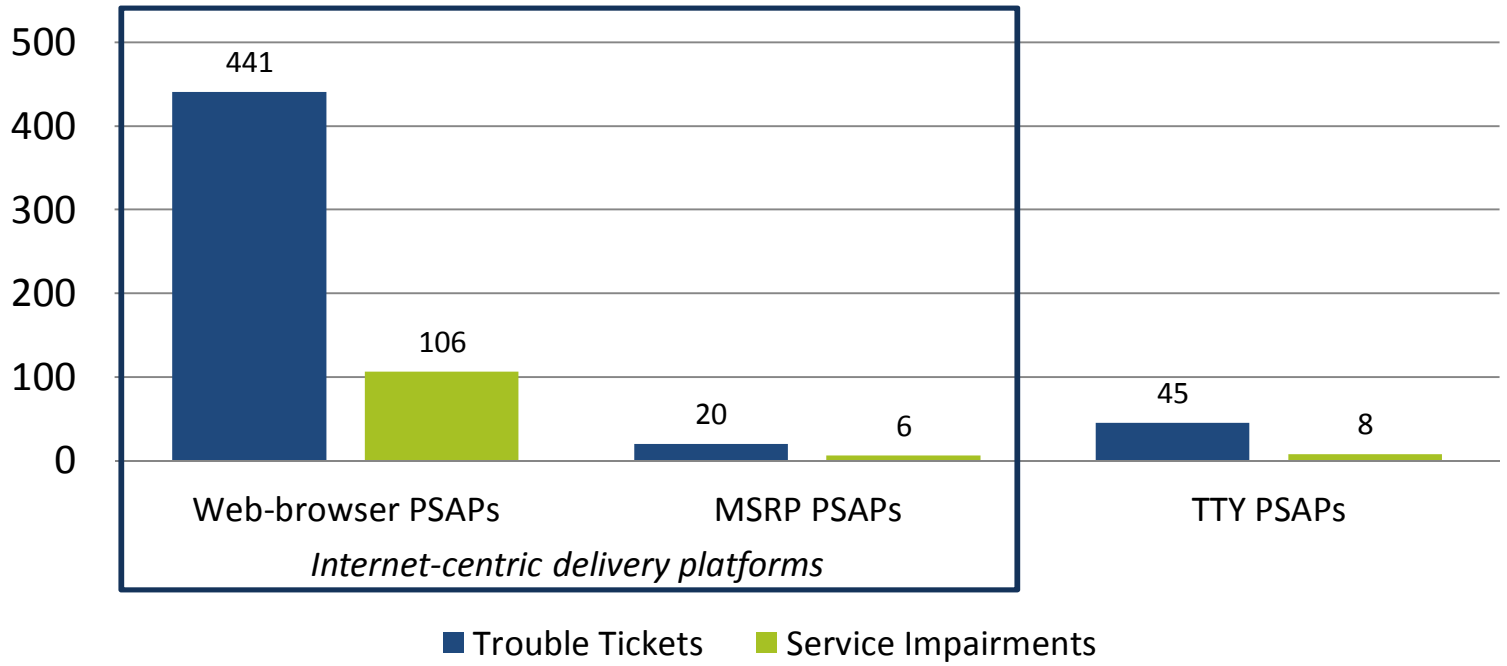
	2012	2013	2014	2015	2016*
GEM	1	31	88	248	335
TTY	0	6	60	149	222
MSRP	0	0	101	150	187
TCC-to-TCC	1	2	15	96	148
Total	**2**	**39**	**264**	**643**	**892**

Fewer PSAPs are deploying text to 9-1-1 service. Of the approximate 6,000 PSAPs, the majority have not requested text to 9-1-1 service and, given how much time has passed since being able to request such service, they do not seem to plan to do so prior to NG9-1-1.

Graphic on the left includes both primary and secondary PSAPs. Chart on the right includes only primary PSAPs

IP-based 911 and the Vulnerabilities of the Public Internet:

Text to 9-1-1 impairment data depicts risk volume of IP platforms



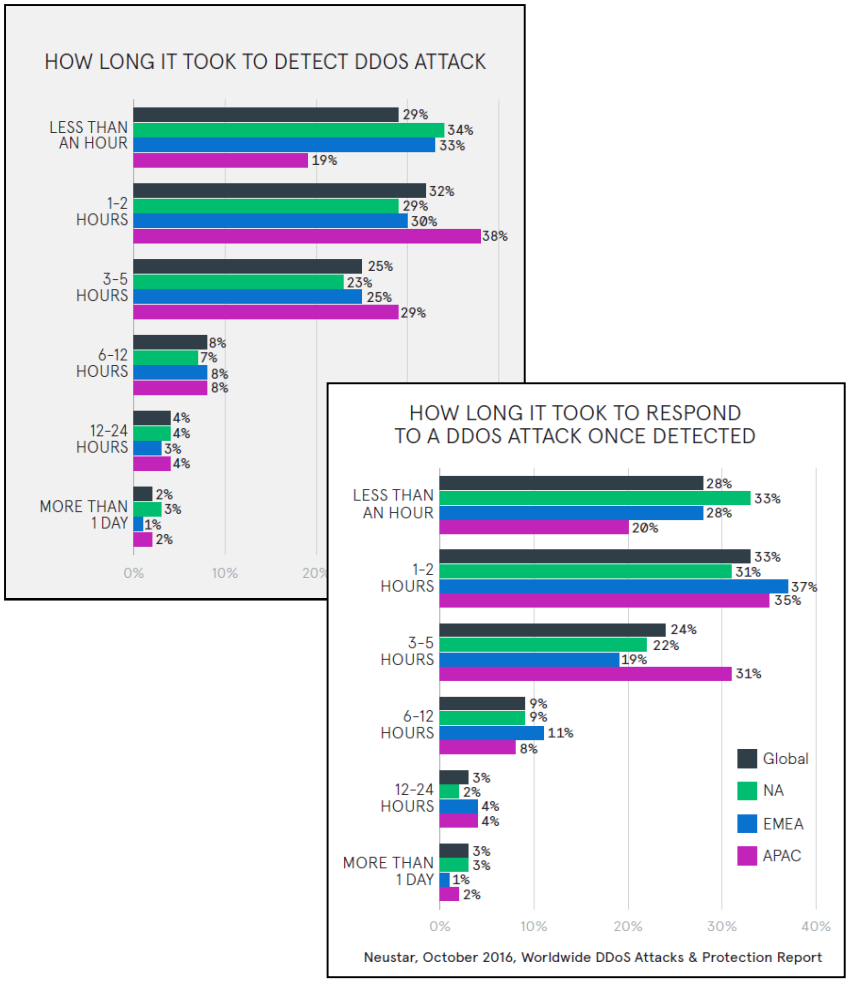
In our experience, all web-browser and MSRP PSAPs that utilize Internet-centric delivery platforms have experienced multiple, complete text-to-911 impairments.

IP-based 911 and the Vulnerabilities of the Public Internet:

Distributed Denial of Service (DDoS) Attacks & Overall Status in North America

Based on an October 2016 Survey of 1,002 directors, managers, CISOs, CSOs, CTOs, and other executives,

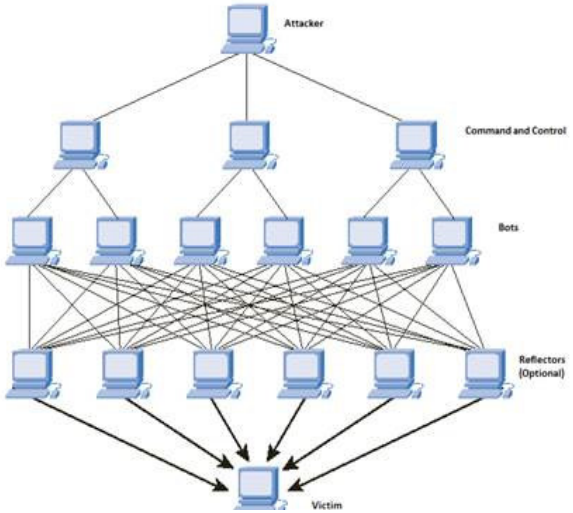
- **85%** of attacked organizations were subjected to multiple DDoS attacks
- **73%** of all organizations interviewed suffered a DDoS attack
- About **1/3** of attacked organizations took less than an hour to detect an attack, but about **2/3** took more than an hour to respond



IP-based 911 and the Vulnerabilities of the Public Internet:

Distributed Denial of Service (DDoS) Attacks – A Comtech 911 Case Study

Our Network Architecture: Comtech uses VPN tunneling at our Text Control Centers (TCCs) for delivery of text-to-911 messages. Those VPN connections over the public Internet do not terminate on the TCCs directly, but to separate, industry-standard VPN gateways.



Is Standards Based: "*SMSC to TCC connectivity may be via a Virtual Private Network (VPN) or other transport methods, or provided through an SMS aggregator.*" (Excerpt from J-STD-110, the only published standard on text-to-911)

Summary of Comtech DDoS events in 2016 YTD:

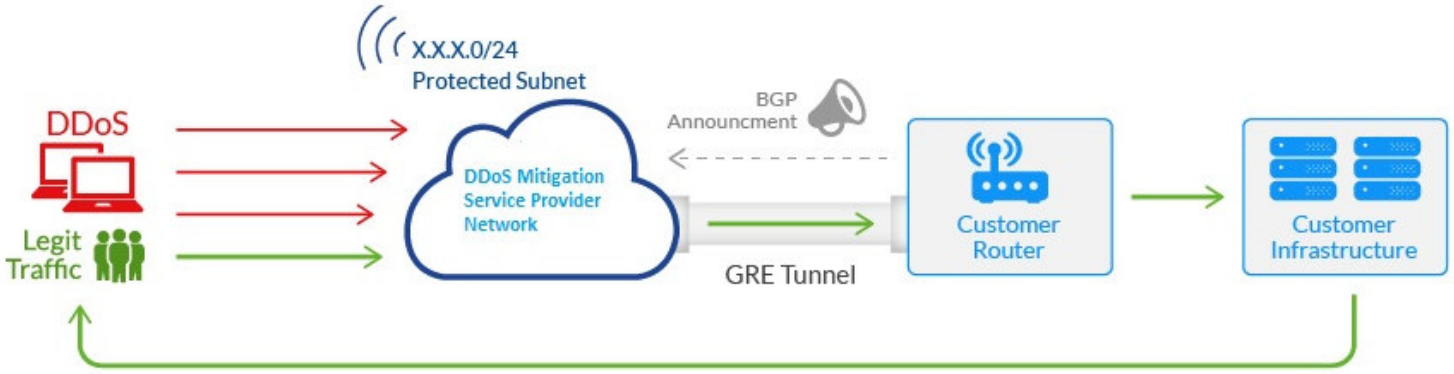
Comtech locations targeted	2
Number of 2016 events	6
First detected event	Jun-8-2016
Most recent perceived event	Sep 17-2016
Number of NORS reports filed	2

IP-based 911 and the Vulnerabilities of the Public Internet:

Distributed Denial of Service (DDoS) Attacks - Current Remediation Status

To protect our public-facing (Internet) services such as web sites and B2B VPNs we have deployed a traffic scrubbing service. The service is provisioned to allow a redirect of traffic in the event of an attack. We monitor networks, systems, and applications for utilization and failure rates. If an anomaly is detected the applicable Internet Service Provider is contacted to validate. The scrubbing service is initiated if an attack has been confirmed.

- Internet circuit monitoring
- DDoS Playbook and Incident Response Procedure
- Traffic scrubbing service

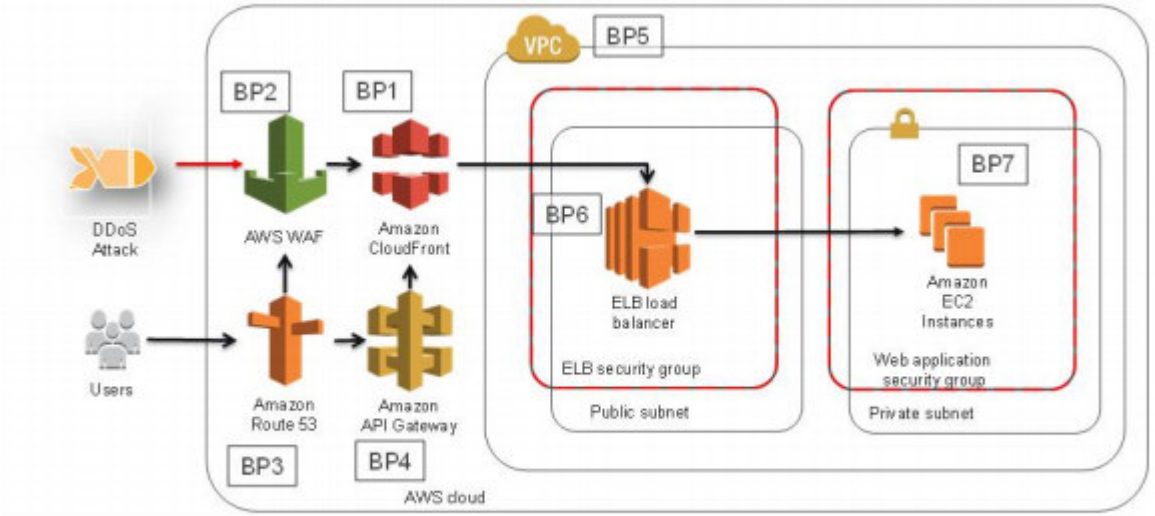


IP-based 911 and the Vulnerabilities of the Public Internet:

Distributed Denial of Service (DDoS) Attacks - Additional Remediation Steps to Consider

To protect the availability of public-facing applications in real time, new architectures are evolving that are not exclusive to cloud service providers. A DDoS resilient architecture might include:

- Always-on (24x7/Automated) WAF (Web Application Firewall), Monitoring, and DDoS mitigation
- Elastic Load Balancing
- Transit capacity, diversity, and location (build in regions that are close to large Internet exchanges/peers)



DDoS-resilient reference architecture

Suggestions for Improving Reliability and Security

1. Encourage Public Safety migration to i3 and delivery of emergency traffic via private circuits to achieve the desired end state of the most reliable and secure 911 national system

2. Encourage PSAPs to incorporate diverse, geo- and vendor-redundant private circuits for last mile connectivity for emergency traffic

3. Encourage PSAPs to conduct Application, Network, Information, and Disaster Recovery audits

4. Encourage PSAPs to keep up with the latest OS software patches on their equipment

Contact Us

Kim Robert Scovill
Vice President, Legal & Regulatory
Comtech Safety & Security Technologies
302-932-9697

275 West Street
Annapolis, MD 21401

kim.scovill@comtechtel.com

www.comtechtel.com